بسم الله الرحمن الرحيم

والحمد لله رب العالمين

والصلاة والسلام على سيدنا محمد النبي الكريم وعلى آله وأصحابه أجمعين

ربنا تقبل منا إنك أنت السميع العليم وتب علينا إنك أنت التواب الرحيم



يقول الله في كتابه العزيز

بسم الله الرحمن الرحيم

" وما أوتيتم من العلم إلا قليلا "

صدق الله العظيم

"رب أشرح لي صدري ويسر لي أمرى واحلل عقدة من لسانى يفقهوا قولي"

اللهم لا علم لنا إلا ما علمتنا إنك أنت العليم الحكيم

أخوكم في الله

م / مصطفى عبده توفيق محمد

جمهورية مصر العربية

الدليل الكبير للأمن

لكى تبقى آمناً



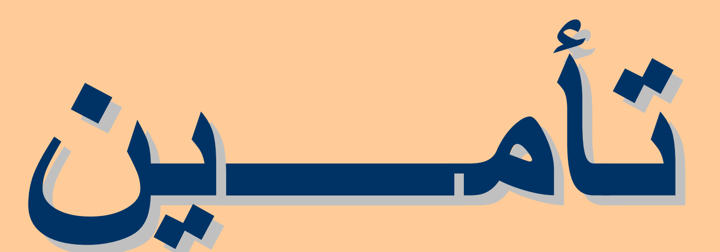
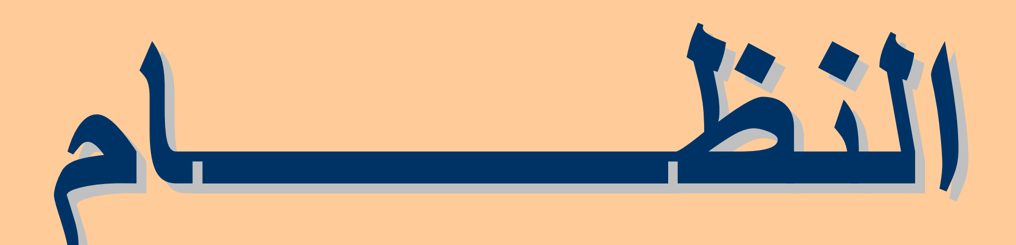
إلى أية درجة تعتبر نفسك خبيراً في أمن حاسوبك؟ الحقيقة أن كثيراً من المستخدمين ليسوا كذلك. وربما جاء جهازك مزوداً، ببرنامج لمكافحة الفيروسات، لكن، هل تم تحديث اشتراكك؟ وهل تشغّل جداراً أمنياً ومن أي نوع؟ هل تجري عمليات فحص منتظمة للتأكد من خلو حاسوبك من كل من البرامج التجسسية وبرامج الإعلانات؟ أم أنك لا تهتم لهؤلاء الهكرة وأولئك المروجين عديمي الضمير إذا أخذوا في البحث بين ملفات حاسوبك عن بياناتك الشخصية؟

كنت دائماً أخبر عن أحدث وأفضل المنتجات الأمنية، لكن الأساس في أية استراتيجية يقوم على الحس السليم، والتشكك الصحّي، والرغبة في التعلم. وحتى إذا كانت مواردك المالية شحيحة، فستجد كثيراً من الخدمات والمنتجات المجانية التي يمكنها مساعدتك في حماية نظامك أو أنظمتك. كما لن يضير وجود بعض الخبراء إلى جانبك، يقدمون لك النصيحة، وهذا هو ما اعتبره دورى.

عزيزى القارئ لقد وضعت فى هذا الكتاب عصارة فكرى فيما يختص بالناحية الأمنية وأخرجت لك ما اسميه بالدليل الأمنى الكبير ليكون لك دليل العون ومرجع فى مواجهة اى مشكلة تختص بالأمن الرقمى فجمعة فيه العشرات من أفضل التلميحات والنصائح، وقسمتها حسب تصنيفها إلى الآتى:-

- تأمين النظام
- تأمين الشبكات السلكية واللاسلكية
- تأمين البريد الإلكتروني
- تأمين التصفح الشبكي
- الأمن من البرامج الخبيثة
- وأخيراً تأمين الأجهزة النقالة

وسواءً كنت مستخدماً مبتدئاً أو محترفاً ، ستجد الكثير من النصائح القيمة لتدعيم دفاعاتك وتعظيم درجة أمنك.


تأمين

النظام

تأمين الحواسيب الجديدة

تكون الحواسيب الجديدة غالباً الضحية الأضعف للهجمات التي تنتقل عبر إنترنت والبريد الإلكتروني، فقبل أن تصل حاسوبك الجديد بإنترنت، تأكد من حمايته باستخدام جدار نار، وتأكد أيضاً من تحديث نظام التشغيل إلى أقصى حد ممكن. وإن كنت تريد تقديم حاسوبا مكتبياً أو نقالاً كهدية لشخص آخر، فعليك تأمينه جيداً قبل أن تعطيه لمستخدم مبتدئ.

ثبت جدار نار عادى

الحل الأمثل أن يكون حاسوبك متصلاً بشبكة مزودة بجدار نار عتادي. فهذا يضمن حماية الأجهزة القابعة خلفه من معظم الهجمات. أما إن لم يكن الحاسوب متصلا بشبكة أصلاً، فيمكنك شراء أحد أجهزة جدر النار. وتوفر كثير من الموجهات المنزلية السلكية واللاسلكية بالفعل نوعا من جدر النار.

ثبت جدار نار برمجي

ستحتاج أيضاً إلى جدار نار برمجي على كل حاسوب متصل بالشبكة، لزيادة قدرتك على حجب هجمات الهكرة، ولحمايتك من التطبيقات التي تسيء السلوك. ويأتي ويندوز إكس بي مرفقاً بحل جزئي؛ لكن، عليك تفعليه حتى تتمكن من الحصول على جدار نار أفضل. فقبل ظهور الإصدارة الخدمية الثانية من هذا النظام، أطلق على هذا الحل اسم "جدار نار الاتصال بإنترنت" (ICF)، وكان مجرد هيكل لجدار نار. غير أن الجدار الذي زودت به الإصدارة الخدمية الثانية من النظام (ويسمى "جدار نار ويندوز Windows Firewall") بدا أفضل بكثير من سابقه، لكنه مازال يمنع الحركة غير المرغوبة الواردة فقط. والحقيقة أنك تحتاج إلى جدار نار مزدوج الاتجاه، مثل Norton Personal Firewall، لمنع حركة المرور غير المرغوبة الصادرة أيضاً، ومنها محاولات برامج التجسس لإرسال بيانات شخصية إلى مبرمجيها.

ثبت حزمة الخدمات الثالثة

عالجت الإصدارة الخدمية الثالثة من ويندوز إكس بي كثيراً من الثغرات الأمنية في نظام ويندوز إكس بي، وحسنت من أداء أداة ترقيع نظام التشغيل. وأكثر الطرائق أمناً لتحديث النظام هي شراء القرص المدمج الخاص بهذه الإصدارة الخدمية من مايكروسوفت، أو تنزيل نسخة كاملة من الحزمة من الموقع downloads.microsoft.com إلى حاسوب تم تحديثه بالفعل، ثم حرقها على قرص مدمج ووضعها على الحاسوب الجديد. وإن قمت بتمكين جدار النار ICF، يمكنك أن تشعر بما يكفي من الأمان للتوجه إلى موقع تحديث ويندوز (www.windowsupdate.com)، وتثبيت الإصدارة الجديدة على الحاسوب الجديد مباشرة.

احزر البرامج الخبيثة

حتى بعد تثبيت برنامج جدار النار، تحتاج إلى اليقظة والانتباه من رسائل البريد الإلكتروني الحاملة للفيروسات، والصفحات الشبكية التي تستغل ثغرات المتصفحات، وبرامج الإعلانات التي قد تثبتها من الشبكة من دون قصد. ثبت برنامجاً لمكافحة الفيروسات وحدثه قبل بدء عملية التصفح، وقبل إعداد برنامج البريد الإلكتروني الخاص بك. واضبط كلاً من برنامج مكافحة الفيروسات ونظام ويندوز بحيث يثبتان التحديثات الأمنية تلقائياً على حاسوبك. وعندما تنقضي فترة اشتراكك في خدمة التحديثات، جددها. فإن ظهرت إصدارة جديدة من برنامج مكافحة الفيروسات، قم بترقية البرنامج. فبرامج مكافحة الفيروسات غير المحدثة لا تمثل أية حماية على الإطلاق!
إذ كان لديك برنامج إعلاني. من المحتمل أن تشتري حاسوباً محملاً ببرامج إعلانية من البداية، لذا يفضل تثبيت منتج قوي لمكافحة برامج التجسس، مثل Spyware Doctor من شركة PC Tools أو Webroot Spy Sweeper. وبعد ذلك، عليك إجراء فحص شامل للحاسب قبل أن تصله بإنترنت.

التنسيق بين الجميع

أسهل طريقة لحماية نفسك وضمان عدم تعارض البرامج التي تثبتها مع بعضها البعض وهو أن تحصل على حزمة متكاملة، تشمل برنامجاً لمكافحة الفيروسات، وآخر لمكافحة برامج التجسس، وثالث لمكافحة البريد التطفلي، وجدار نار.

حماية بأرخص الوسائل

توجد كثير من البرامج المجانية الجيدة لمكافحة الفيروسات وبرامج جدر نار، مثل avast!4Home Edition. وبصفة عامة، ستجد أن هذه البرامج مخصصة للاستخدام الشخصي، ولا يسهل ضبطها تماماً مثلما تستطيع أن تفعل مع المنتجات التجارية. (انظر قسم "الموارد الشبكية" في هذا الدليل).

تقييد الوصول

يقدم المكون "حسابات المستخدمين" (User Accounts)" في نظام ويندوز إكس بي مستويين لأمن المستخدمين: مستوى المستخدم المدير، ومستوى المستخدم المحدود. ويسمح حساب المدير لك بتنفيذ أي إجراء على حاسوبك، وهو ما يجعلك في وضع المخاطر بالتعرض لأية برامج خبيثة قد تثبت بعض الشيفرات على حاسوبك بكل حرية. أما الحساب المحدود، فلا يسمح بتثبيت أية برامج أو بإحداث تعديلات في إعدادات النظام.

قيد نفسك

يسألك ويندوز إكس بي افتراضياً عن اسم مستخدم أثناء تركيبه، ويجعل لهذا الاسم خصائص حساب المدير كاملة، ويقلع الحاسوب مباشرة إلى هذا الحساب بعد ذلك فصاعداً. لكن، يمكنك إعداد حساب مقيد من خلال النقر على قائمة "ابدأ|لوحة التحكم|حسابات المستخدمين" (Start|Control Panel|User Accounts) واختيار "إنشاء حساب جديد" (Create New Account) وإعطاء هذا المستخدم الجديد اسماً. انقر على "التالي" (Next)، واختر "مستخدم محدود" (Limited User) في صندوق "نوع المستخدم" (User Type)، ثم انقر على زر "إنشاء حساب" (Create Account). واستخدم حساب المستخدم المحدود هذا للأنشطة اليومية.

ضع كلمة سر او "مرور"

لمزيد من الأمان، خصص كلمة سر لكل حساب يتمتع بخصائص المدير. وفي صندوق حوار "حسابات المستخدمين" (User Accounts)، انقر فوق اسم المستخدم واختر "إنشاء كلمة سر" (Create a Password). اتبع إرشادات البرنامج الإرشادي، وأضف كلمة سر للحساب. ولا تستخدم كلمة سر واضحة، مثل "password" أو "admin" أو اسم المستخدم نفسه.

أوصد الأبواب

بعضهم لا يرغب في وضع كلمة سر لأنها تبطئ عملية الدخول إلى النظام. ولكن الحماية بكلمة السر ضرورة مطلقة. وعلى أي حال، إن كنت مطمئنا لوجود حاسوبك في مكان آمن، يمكنك استخدام أدوات القوة Power-Toy TweakUI من مايكروسوفت www.microsoft.com/windowsxp/downloads
للدخول إلى حساب معين تلقائياً. انقر على العلامة الموجودة إلى جانب كلمة Logon، واختر Autologon، ثم اختر Logon automatically at system startup، وحدد اسم مستخدم وكلمة سره. لاحظ أن المكتب ليس مكاناً آمنا. وإنما ننصح بهذه الطريقة فقط إن كنت تثق بكل من يقيمون معك في المنزل وزوارك فيه، وإن كان حاسوبك في موضع آمن دائماً.

الإصلاح السريع

للأسف، فإن حساب المستخدم المحدود يجعل بعض التطبيقات، مثل الألعاب، صعبة أو مستحيلة التشغيل. لكن، يمكنك الدخول كمستخدم محدود وتشغيل البرامج غير المتوافقة معه باستخدام خيار Run with different credentials. ثبت التطبيق أولاً، وقد يعترض ويندوز إذا حاولت تركيبه من الحساب المحدود، وفي هذه الحالة، عليك تسجيل الخروج، والعودة باسم حساب المدير، أو قد يسألك فقط عن اسم حساب المدير وكلمة سره. وبعد اكتمال عملية تثبيت البرنامج وتشغيله، اخرج من حساب المدير وسجل الدخول بحساب المستخدم المحدود. وسيعمل التطبيق بشكل جيد، فإن فشل، انقر بالزر الأيمن على اختصاره أو على اسمه في قائمة البرامج، واختر "خصائص" (properties)، وانقر على زر "خيارات متقدمة" (Advanced) في لسان التبويب "اختصار" (Shortcut). والآن، ضع

علامـة فـي المربـع المقابـل لخيـار "التـشغيل بمـؤهلات اعتمـاد مختلفـة" (Run with Different Credentials) وانقر على "موافق" (Ok).
لاحظ أن ويندوز لن يسمح لمستخدم محدود بتغيير اختصار يشارك فيه كل المستخدمين.
فإن ظهرت رسالة الخطأ "الوصول ممنوع" (Access denied) عندما تنقر زر موافق، ألـغ التعديلات، واسحب الاختصار بـالزر الأيمن إلـى سطح المكتب، واختر نـسخ Copy. والآن، عدل الاختصار المحلـي النـاتج بالطريقة المذكورة سابقاً. وعندما تنقر نقراً مزدوجاً على هذا الاختصار، سيظهر مربع حوار لتسجيل دخولك بحساب يتمتع بصلاحيات المدير.

التحصن داخل المناطق الأمنية

حتى إذا لم يكن إنترنـت إكسبلورر هو متـصفحك الافتراضـي، فـإن محركـه يـستخدم فـي كل شيء تقريبا علـى نظـام ويندوز بـدءاً من مدير الملفـات "مستكشف ويندوز" (Windows Explorer) وحتـى "سطح المكتب الفعال" (Active Desktop). وهكذا، حتـى فـي حـال عـدم اسـتخدامه، فإنـك لا تـزال معرضـاً لأي تهديـد شـبكي يـستغل الثغرات الأمنيـة فـي هـذا البرنـامج. وننصح باستخدام المناطق الأمنية لإدارة التعامل مع مواقع إنترنـت، ولكـن لا يتـاح الحاسـوب المحلـي أو "جهـاز الكمبيـوتر" "My Computer" افتراضـياً داخـل إعـدادات المناطق. لكن يمكنك إعداد قيمة في سجل النظام Registry لجعله متاحاً.
أغلـق جميـع نوافـذ المتـصفح ونوافـذ مستكـشف النوافـذ أو نوافـذ "جهـاز الكمبيـوتر" (My Computer)، ثـم افـتح برنــامج تحريـر الـسجل "ابـدأ|تـشغيل" (Start|Run) ثـم أدخـل regedit قبل الضغط على زر الإدخـال. توجـه إلـى مفتـاح السجل: HKEY CURRENT USER\Software\Microsoft\Windows\Current Version\Internet Settings\Zones\0. انقـر بـالزر الأيمـن علـى هـذا المفتـاح واختـر "تـصدير" (Export) لإنشاء ملف سجل REG file يمكنك تشغيله للتراجع عن أية تعديلات تدخلها إذا لزم الأمر.
حدد موضـع القيمة التـي تحمل الاسم Flags، وانقر نقراً مزدوجاً عليهـا. وفـي نافـذة التحريـر الخاصة بها، غير قيمتها إلى "1". انقر على "موافق"، وأغلق برنامج تحرير السجل.
وبعد إدخـال هـذا التغييـر، توجـه إلـى "لوحـة التحكم" (Control Panel) وافـتح "خيـارات إنترنـت" (Internet Options)، واختر قسم "الأمن" (Security). اختر منطقة المحتوى: My Computer (ربما كان عليك الانتقال بسطر الإزاحـة إلـى اليمين قليلا للعثور عليهـا)، ثم انقر فوق "مستوى مخـصص" (Custom Level) لإدخـال التغييـرات التـي تريدها علـى هذه المنطقة. كن حذراً، فالتغييرات الأمنية التي تدخلها هنا قد تؤثر علـى الطريقـة التـي تعمـل بها بعض البرامج. وعندما لا تكون متأكداً مما تفعله، اضبط إنترنت إكسبلورر بحيـث ينبهـك عند كل حدث يثير التساؤل بدلا من منعه مباشرة.

التراجع زمنياً

استخدم وظيفة "استعادة النظام" (System Restore): تسمح هذه الوظيفة (المتوفرة في ويندوز ميلينيوم وإكس بي) بإعادة إعدادات النظام والملفات المهمة إلى حالة سابقة إذا أدى تركيب بعض البرامج أو إزالة تركيبها إلى مشكلات. وتعدّ هذه الأداة نقاط استعادة تلقائية بشكل منتظم، كما تنشئ نقاطاً إضافية قبل تثبيت التطبيقات، وبرامج القيادة المختلفة. وعندما لا تستطيع أدواتك الأمنية تخليصك من إصابة فيروسية أو هجوم معين، جرب وظيفة استعادة النظام لإعادة نظامك إلى الحالة التي كان عليها في وقت سبق تركيب التطبيق الخبيث.
وللتأكد من تشغيل وظيفة استعادة النظام، توجه إلى لوحة التحكم واختر "النظام" (System)، ثم اختر قسم "استعادة النظام" (System Restore) وعاين الوضع هناك.

وظيفة استعادة النظام فى نظام التشغيل ويندوز2000

لا يوفر نظام التشغيل ويندوز 2000 وظيفة استعادة النظام. ولكن، يمكنك محاكاة كثير من وظائفها. ففيه برنامج نسخ احتياطي (Start|Programs|Accessories|System Tools|Backup) يتضمن وظيفة باسم System State في قسم Backup. وهي تسمح بإنشاء نسخة احتياطية لملف الإقلاع boot، ولقاعدة البيانات الخاصة بتسجيل الأصناف COM ، وأيضا لملف سجل النظام.

تعطيل وظيفة استعادة النظام مؤقتاً فى إكس بي

المؤسف أنه لا يمكن لأدوات مكافحة الفيروسات ومكافحة التجسس إزالة الإصابات المسجلة في نقاط الاستعادة، وهذا يعني أنك حتى لو أزلت بعض البرامج الخبيثة، فإن إعادة نظامك إلى نقطة زمنية سابقة قد تعني إعادة الإصابة أيضاً. وقد رأينا أيضاً أن نقاط الاستعادة المصابة تجعل أجراس التحذير في برامج الأمن تنطلق مع كل عملية فحص للجهاز. ولمنع هذا، عليك تعطيل وظيفة استعادة النظام.
في لسان التبويب "استعادة النظام" الذي تصل إليه من "النظام" في لوحة التحكم، اختر "إيقاف تشغيل استعادة النظام على كافة محركات الأقراص" (Turn off System Restore on all drives). وسيؤدي هذا إلى مسح جميع نقاط الاستعادة السابقة. وبعد إتمام عملية التنظيف وإزالة البرامج الخبيثة، أعد تشغيل وظيفة استعادة النظام، بإزالة العلامة عن ذلك الخيار الأخير.

استخدام الوضع الآمن

يعدّ تشغيل النظام في الوضع الآمن إحدى الطرائق المعدودة لاستعادة التحكم في النظام بعد تعطله، أو بعد تعرضه لهجمة فيروسية أو تجسُسية. ففي العادة، يمنعك ويندوز من حذف أية ملفات مستخدمة حالياً (بما فيها البرامج الخبيثة)، إذ تشغّل هذه البرامج الخبيثة ذاتها غالباً لدى بدء تشغيل الحاسوب. لكن الوضع الآمن يتجاهل كثيراً من برامج القيادة وغيرها من برامج بدء التشغيل، ومن خلال التوجه إلى هذا الوضع، قد تتمكن من إزالة التطبيقات المسيئة. (وقد وجدة أيضا أن مجرد الدخول إلى الوضع الآمن، ومن ثم إعادة التحميل إلى الوضع الطبيعي قد تجعل النظام غير المستقر أكثر استقرارا.)

ولدخول الوضع الآمن، عليك إقناع ويندوز بعرض قائمة بدء التشغيل. وتبعا لنظام التشغيل الذي تستخدمه، تعرض هذه القائمة الوضعين الطبيعي والآمن، وأحياناً تعرض أيضا الوضع الآمن مع تمكين الشبكة، ووضع محث الأوامر، وخيارات أخرى.

الدخول إلى الوضع الآمن بالمفتاح F8

يمكنك الدخول إلى قائمة بدء التشغيل بالضغط على مفتاح F8 من لوحة المفاتيح أثناء تحميل الحاسوب، أو باستخدام برنامج تهيئة النظام MSConfig (وهي لا تتوفر في ويندوز 2000).

وفي العادة، يمكنك دخول الوضع الآمن بالضغط على المفتاح F8 بعد توصيل الطاقة بالحاسوب. لكن بعض الأنظمة قد تحثك على الضغط على هذا المفتاح في وقت محدد أثناء عملية الإقلاع بعد تلقي إشارة معينة، مثل خط صغير أو مربع في الركن العلوي الأيسر من الشاشة، أو بصوت تنبيه. وأيا كانت الإشارة، فعندما تتلقاها، اضغط F8. فإن كان نظام بيوس لديك قد ضبط على وضع الصمت، فقد لا ترى هذه الإشارة.

دخول الوضع الآمن بطريقة MSConfig (مع ويندوز إكس بي)

إن كنت تستخدم ويندوز إكس بي، اختر Run من قائمة Start، واكتب msconfig، واضغط زر الإدخال. اختر قسم BOOT.INI، وقم بتمكين خيار /SAFEBOOT وانقر موافق مرة أخرى. وإن كنت ستحتاج إلى وصلة شبكة أو وصلة إنترنت، ضع علامة أمام الخيار NETWORK هنا أيضاً. وعندما يطلب منك النظام إعادة التشغيل، انقر Restart، وسيتم تشغيل الحاسوب في الوضع الآمن. وللإقلاع في الوضع الطبيعي، أعد فتح برنامج MSConfig، واختر قسم BOOT.INI، وأزل العلامة الموضوعة أمام الخيار /SAFEBOOT، ثم اختر لسان التبويب "عام" (General)، وضع علامة على الخيار "بدء تشغيل عادي" (Normal Startup).

توسيع نطاق رؤيتك

غالبا ما تستخدم ملفات البرامج الخبيثة امتدادين للملفات. فافتراضياً، يخفي ويندوز امتدادات الملفات؛ وقد تساعد هذه الوظيفة البرامج الخبيثة على التخفي حتى تجعلك تعتقد أنها آمنة ويمكنك فتحها. مثلاً، يوجد فيروس يسمى prettywoman.jpg.exe، و وهو يظهر لديك باسم الملف prettywoman.jpg، وكأنه ملف صورة، وعليك تغيير إعداداتك حتى ترى الامتدادات الحقيقية.

في نظامي ويندوز إكس بي و2000، افتح نافذة "جهاز الكمبيوتر" (My Computer)، ثم انقر على "أدوات|خيارات المجلد" (Tools|Folder Options). اختر لسان التبويب "عرض" (View)، ابحث عن الخيار "إخفاء ملحقات الملفات لأسماء الملفات المعروفة" (Hide extensions for known file types) وأزل العلامة الموضوعة أمامه.

تأمـين الشبــكات السلـــــكية واللاسلــــــكية

ما مدى الأمان الذي تتمتع به؟

إجراء عملية فحص

تعمل أدوات فحص إمكانية تعرض حاسوبك للمخاطر بالتدقيق في الحواسيب المتصلة بشبكة معينة للتعرف على الثغرات الأمنية المحتملة فيها، وقد يعطيك بعضها إرشادات لتدارك هذه المشكلات. وتتوفر كثير من هذه البرامج تجارياً وتقدم نتائج ممتازة، منها: Retina من eEye (www.eeye.com)، وISS Internet Scanner (www.iss.net)، و AppDetective من Application Security (www.appsecinc.com)، والتي تفحص الشبكة بحثاً عن مجموعة كبيرة من المشكلات المعروفة، ويتم تحديثها مع اكتشاف أية مشكلات جديدة. ويمكنك تحديد نظام بعينه لفحصه باستخدام هذه الأدوات، أو عندما تحدد لأي منها نطاق عناوين IP، يمكنها العثور على جميع الأنظمة في شبكتك وفحصها.
تعتبر أسعار هذه الأدوات باهظة بالنسبة للشبكات المنزلية. وبدلا منها، يمكنك تجربة برنامج الفحص NeWT، وهو أداة مجانية من شركة Tenable Network Security (www.tenablesecurity.com)، كما تعرض مايكروسوفت أيضا أداة مجانية، هي Microsoft Baseline Security Analyzer (support.microsoft.com) والتي تفحص نظماً مستقلة بعينها، أو نظماً متصلة شبكيا للتعرف على التهيئات الخاطئة الشائعة بها، وكذلك التحديثات الأمنية المفقودة. فإن كنت تدير شبكة في العمل، عليك استخدام هذه الأدوات المجانية بالإضافة إلى أحد برامج الفحص التجارية.

افحص شبكتك من الداخل ومن الخارج

تتم عمليات الفحص التي تجري داخل الشبكة بحثا عن أوجه الخطر التي قد تأتي من جانب مستخدم دخل بالفعل إلى الشبكة. فإن كنت قد ثبتّ جداراً نارياً، فستكون شبكتك محمية من الكثير من المخاطر الخارجية. قم بتشغيل أداة الفحص من خارج الشبكة، وأخبرها أن تفحص عنوان IP الخارجي الخاص بك. ألق نظرة على المنافذ المفتوحة على نظامك، وتأكد أنها جميعاً تستخدم مع التطبيقات التي تريدها.

توخ الحذر

قد تعطيك برامج الفحص سيلا من رسائل التحذير، وكثير منها لا يقدم لك أكثر من بلاغ بأنك فعلت شيئا معيناً (مثل فتح منفذ 80 على مزودك الشبكي) والذي قد تكون قصدت فتحه فعلاً. لذا، لا تفترض أن هذا البرنامج يعرف أكثر منك، خاصة عندما يعطي التحذير أولوية منخفضة. خذ النصيحة من هذه البرامج باعتبارها مقترحات، وليست أوامر.

شبكات لاسلكية

استخدام البروتوكول WPA

حتى أولئك الذين صمموا البروتوكول WEP (Wired Equivalency Privacy)، وهو بروتوكول الأمن اللاسلكي الخاص بالجيل الأول من الأجهزة اللاسلكية، يعترفون بأنه بروتوكول ضعيف يسهل خداعه. أما بروتوكول الجيل الثاني WPA (Wi-Fi Protected Access) فهو حل أفضل بمراحل، ولكنه ليس متاحا بالضرورة لأجهزة واي فاي القديمة التي قد تتوفر لديك. فمثلاً، ضمنت Linksys دعما لهذا البروتوكول في كل أجهزتها التي تعتمد المعيار g802.11، لكنها لم تضفه إلى مجموعة من أجهزتها التي تعتمد المعيار الأقدم b802.11، وعليك تحديث أجهزتك حتى تدعم هذا البروتوكول. ويشتمل هذا البروتوكول على وضعين: وضع مخصص لمجال الأعمال enterprise، يمكن للمستخدمين فيه إدخال أسماء مستخدمين وكلمات سر بمراجعتها مزود خاص، ووضع شخصي Personal، حيث يمكن للجميع استخدام كلمة سر واحدة مشتركة. وتستخدم هذه الكلمة كمفتاح لتشفير كل البيانات على الشبكة. وفي التجارب، وجدوا أنه يمكن لجميع المستخدمين المنزليين، وجميع الأعمال الصغيرة تقريباً الاكتفاء بوضع كلمة السر المشتركة.

توجد إصدارة حديثة نسبياً من بروتوكول WPA تسمى WPA2 تطبق تشفيراً أقوى مما تستخدمه الإصدارة السابقة، وقد بدأت تظهر في المنتجات الحديثة. وهذه التحسينات تعد أكثر مما يحتمله المستخدمون المنزليون، ولكن، الإصدارة الجديدة تمتاز بأنها تتوافق مع البروتوكول WPA، لذا لا يوجد مبرر لعدم شرائها. وللحصول على أفضل حماية ممكنة، استخدام كلمة سر لا تقل عن 20 حرفاً، واكتبها في مكان آمن.

تجنب التطفل عبر ماسينجر ويندوز

إن كنت تستخدم ويندوز إكس بي أو 2000 وتتصل مباشرة بإنترنت، قد تقع ضحية للنوافذ المنبثقة الخاصة بخدمة ويندوز ماسينجر. ولا ترتبط هذه الخدمة بأي من تطبيقات التراسل الفوري، ولكن بخدمة شبكية تدعى Net Send.
ظلت خدمة رسائل شبكة Net Send تستخدم من قبل مديري الشبكات لإرسال رسائل منبثقة لكل المستخدمين على هذه الشبكات (مثل الرسالة "المزود سيفصل خلال 5 دقائق، لذا، احفظ ما تفعله، وأنهه")، وأيضا للسماح للمستخدمين بإرسال ملاحظات إلى بعضهم.
تعمل هذه الخدمة افتراضياً، على نظامي ويندوز إكس بي و 2000 عندما تشغل الحاسوب، ونتيجة لذلك، فعندما تتصل بإنترنت، فإن كل من يعرف عنوان IP الخاص بك يمكنه إرسال رسالة منبثقة تبدو كتحذير من ويندوز، وليس كإعلان. ويجري بعض مرسلي الرسائل التطفلية فحص على سلسلة من عناوين إنترنت للعثور على الحواسيب التي تعمل عليها هذه الخدمة. وعندما يعثرون على أحدها، يرسلون رسالة له.

عطل وظيفة Net Send

في نظامي ويندوز 2000 وإكس بي، يمكنك تعطيل وظيفة خدمة الماسينجر Messenger Service بالنقر على زر "ابدأ" (Start)، ثم اختيار "تشغيل" (Run) وكتابة Services.msc، ثم الضغط على زر الإدخال. وفي نافذة الخدمات التي ستظهر، انتقل إلى المادة الخاصة بخدمة الماسينجر Messenger. انقر نقراً مزدوجا لفتح نافذة الخصائص. انقر أولاً زر "إيقاف" (Stop) لإنهاء الخدمة، وبمجرد ظهور ما يشير إلى أنها قد توقفت، انقر فوق مربع "طريقة بدء الخدمة" (Startup Type)، واختر "تعطيل" (Disabled). والآن، انقر على موافق، وستتم إعادتك إلى نافذة الخدمات، وستجد أن نافذة خصائص خدمة الماسينجر تحوي كلمة ""معطلة" (Disabled) في خانة "طريقة بدء الخدمة" (Startup type). أغلق النافذة وبهذا تنتهي المهمة.

أو احتفظ بها تعمل

يمكن للتعديل السابق أن يلغي المشكلة تماماً، على الرغم من أنه قد يقف عثرة في طريق برامج أخرى شرعية تستخدم وظائف التنبيه، مثل برامج مكافحة الفيروسات وبرامج ترتيب مهام الطباعة print spoolers أو أجهزة UPS.
فإن وجدت أنك مضطر للاحتفاظ بهذه الخدمة، يمكنك منع الرسائل الخارجية باستخدام جدار ناري. وعند استخدام جدار ناري برمجي أو عتادي، قم بتعطيل الحركة الواردة التي تعتمد على الإذاعة عبر بروتوكولي NetBIOS وUDP. وعند إعداد جدار ناري شخصي، قد تحتاج إلى إنشاء استثناءات لشبكتك الداخلية الخاصة بك، أو لأجهزة معينة تشاركها بياناتك.

العمل على السلسلة

تندرج بعض البرامج التي تسعى للسيطرة على المتصفحات ذاتها في المكون "مقابس ويندوز" (Windows Sockets) – وهي آلية تستخدمها التطبيقات لإجراء اتصال بإنترنت وعندما تتم إزالة هذه البرامج الخبيثة، فإنها تترك هذا المكون مكسور الحماية وغير قادر على الاتصال.

ويحوي البروتوكول Winsock 2، الذي يتم تثبيته بواسطة النسخ المحدثة من إنترنت إكسبلورر، والمبيت في ويندوز إكس بي، وظيفة تسمى "خدمة مزود الخدمات الطبقي" (Layered Service Provider)LSP ، والذي يسمح لمصممي البرامج المستقلة بإدخال شفراتهم الخاصة (لإجراء مراقبة أو ترشيح للمحتوى) في دفقة بيانات Winsock. وتستخدم الوظيفة عينها برامج التجسس أيضاً لتسهيل عمليات المراقبة التي تجريها. وعندما تتم إزالة برنامج شرعي (مثل Net Nanny أو Cybersitter)، فإنه يعدل آلية Winsock بإزالة الشفرة التي أدخلها. ولكن برامج التجسس لا تقدم هذه الخدمة الطيبة.

وإذا كسرت حماية Winsock، ستجد أنك تتمكن من استخدام برنامج التراسل الفوري، بخلاف برامج البريد الإلكتروني، أو برامج التصفح الشبكي. وهذا الأسلوب الذي تعتبره غريباً يجعل عملية الإصلاح صعبة لأنك متصل بإنترنت، وأيضا لديك عنوان IP ولكن المتصفح لا يعمل.

وأفضل وسيلة لإصلاح مشكلة السلسلة المكسورة هو استخدام برنامج مجاني يسمى LSP-Fix. وهذا البرنامج صمم مبدئيا للعمل على نظام ويندوز 98، على الرغم من أنه يعمل على نظم ميلينيوم وإكس بي و2000 أيضاً. وهو متاح عبر الموقع Counterexploitation، وهو موقع شبكي مخصص للتعرف على برامج التجسس، وبرامج الإعلانات، وغيرها من البرامج الخبيثة، وإزالتها، على العنوان www.cexx.org/lspfi x.htm. ويعمل هذا البرنامج من خلال إعادة وصل الطبقات المفصولة في كومة Winsock. وفي معظم الحالات، يمكنه إصلاح الضرر الناتج من دون إحداث مشكلات إضافية.

تأمــين

البريــــــد

الإلكــــتروني

لا للمعاينة الأولية

كلنا نعرف أنه لا يجب فتح المرفقات غير المعروفة، غير أن ترك وظيفة المعاينة الأولية لرسائل البريد الإلكتروني Preview في برنامجي آوتلوك، وآوتلوك إكسبريس يجعل الرسائل التي قد تجلب الإصابة لحاسوبك بمختلف المخاطر تفتح تلقائياً. لاحظ أنك، إن قمت بتثبيت الإصدارة الخدمية الثالثة لنظام ويندوز إكس بي (كما نصحنا بذلك في القسم الأول من هذا الدليل)، فإن كلا من آوتلوك ونظام التشغيل لا يسمح بعرض كثير من العناصر المسببة للمشكلات في نافذة المعاينة الأولية، ولكن، من الأفضل أمنياً أن يتم تعطيل هذه الوظيفة تماماً.

في برنامج آوتلوك إكسبريس، اختر View|Profiles|Preview Pane وعطلها.

في آوتلوك 2000، اختر View|Preview|Pane (وستجد أنها من نوع زر الاختيار القلاب، فانقر عليه مرة لتشغيله ومرة أخرى لتعطيله).

في آوتلوك 2003، اختر "عرض|جزء القراءة|إيقاف التشغيل" (View|Reading Pane|Off).

لا للمرفقات

امنع المرفقات في آوتلوك: لعل عدم فتح المرفقات هو السبيل الأفضل لمنع خطر الإصابة بالفيروسات. وضبطت برامج البريد الثلاثة: آوتلوك 2003 وآوتلوك 2002 وآوتلوك إكسبريس الإصدارة السادسة لمنع المرفقات الخطرة تلقائياً؛ وفي آوتلوك إكسبريس، يمكنك تعطيل وظيفة المنع هذه، غير أنه في آوتلوك 2003، سيظل المنع سارياً في كل الأحوال. كما يمكنك تحديث برنامجي آوتلوك 98 أو آوتلوك 2000 حتى يشملا على وظيفة منع المرفقات.

عطل المرفقات في آوتلوك إكسبريس- الإصدارة السادسة: إن كنت تستخدم آوتلوك إكسبريس الإصدارة السادسة، وكنت قد عطلت وظيفة إظهار الامتدادات في ويندوز، انقر "أدوات" (Tools) ثم اختر "خيارات" (Options). اختر قسم "أمان" (Security)، وضع علامة في المربع المجاور للخيار "عدم السماح بحفظ المرفقات أو فتحها التي من المحتمل أن تكون فيروساً" (Do not allow attachments to be saved or opened that could potentially be a virus).

التحذير المبكر

في آوتلوك إكسبريس، ضع علامة في المربع الخاص بالخيار "التحذير عند محاولة إرسال أحد التطبيقات الأخرى بريداً باسمي" (Warn me when other applications try to send mail as me) لمزيد من الحماية الأمنية من خلال تنبيهك لدى محاولة التطبيقات الأخرى إرسال بريد كما لو كان صادراً من قبلك.

أضف إلى قائمة المرفقات المحظورة

ماذا عن الملفات من نوع ZIP وPIF وغيرها من هيئات الملفات التي قد تخفي برامج خبيثة؟ لا يتم حظر هذه الأنواع افتراضياً، ولكن، يوجد موضوع في قاعدة المعرفة الأساسية الخاصة بمايكروسوفت على الموقع support.microsoft.com/kb/837388 يصف طريقة إضافة المزيد من الامتدادات لقائمة الملفات المحظورة الخاصة ببرنامج آوتلوك، ولكنها طريقة لا تعمل للأسف على برنامج آوتلوك إكسبريس. ويتطلب هذا الأسلوب تحرير سجل النظام، ويصلح على الأرجح لكل من آوتلوك 2003 و 2000 و2002.
وهذه الخطوات مناسبة للمستخدمين المنزليين (الذين لا يعملون في بيئة تعتمد على مزود Exchange) باستخدام برنامج آوتلوك 2003. وبالنسبة لمستخدمي آوتلوك 2000، يمكنهم التعويض بـ 9.0 عن 11.0 في المفتاح HKEY. أما بالنسبة لمستخدمي آوتلوك 2002، يمكنهم التعويض عن القيمة عينها بـ 10.0. وننصح بعمل نسخة احتياطية من هذا المفتاح قبل التعديل.
انقر على "ابدأ|تشغيل" (Start|Run)، واكتب regedit وانقر على موافق. توجه إلى المفتاح التالي وانقر عليه:
HKEY_CURRENT_USER\Software\Microsoft\Office\11.0\Outlook\Security. ومن قائمة "تحرير" (Edit)، أشر إلى "جديد|قيمة سلسلة" (New|String Value). اكتب Level1Add اسما للقيمة الجديدة، ثم انقر على "موافق". ومن قائمة "تحرير" (Edit) أيضاً، انقر على "تعديل" (Modify)، ثم اكتب < واكتب كل امتدادات الملفات التي تخشى أن تحمل فيروسات (مفصولة بالفاصلة المنقوطة، لا الفراغات)، ثم اكتب &gt؛ يمكنك مثلاً كتابة .zip;.pif إذا كنت تريد حظر هاتين الهيئتين من الظهور في رسائل البريد الإلكتروني إذا وصلتا كملفات مرفقة. وستبدو القيمة النهائية كما يلي: <zip;.pif.>
إزالة حظر الملفات: إن احتجت لإتاحة الوصول إلى مرفق تم حجبه، يمكنك استخدام المفتاح Level1Remove. وننصحك بالتوجه إلى موقع أنظمة Slipstick Systems (www.slipstick.com) للحصول على تعليمات وقائمة متكاملة بالامتدادات المحظورة، وأيضا قائمة بالأدوات التي تسمح لك بإضافة حظر المرفقات وإزالته بدون تحرير سجل النظام.

الإعادة إلى المرسل

التمثيليات الخادعة: أحد الآثار الجانبية غير المرغوبة للديدان الحديثة هو سيل البريد الذي لم يتم تسليمه. فكثير من الفيروسات تستخدم رسائل تحمل العنوان "لا يمكن تسليمه Undeliverable" أو ما شابه حتى تغري المستخدم بفتحها وإصابة حاسوبه. كذلك، فإن فيروسات البريد الإلكتروني تتعمد تزييف عنوان الرد عندما ترسل ذاتها إلى قائمة تم حصادها. ويؤدي هذا إلى منع رسائل عدم التسليم الشرعية من تنبيه المستخدم إلى وجود الفيروس على حاسوبه في حين يغرق صندوق الوارد الخاص بمالك العنوان الذي تم استغلاله برسائل عدم التسليم التي لا تخصه. وفي كل من الحالتين، قم بحذف هذه الرسائل من دون فتحها.

راجع ترويسات الرسائل

إذا كنت تعتقد أن رسالة ما قد تكون من عنوان شرعي، انقر عليها بالزر الأيمن في صندوق الوارد الخاص بأوتلوك، واختر "خيارات" (Options) لمطالعة الترويسات (لا تنقر نقراً مزدوجاً، لئلا تفتح الرسالة). وفي آوتلوك إكسبريس، انقر بالزر الأيمن على الرسالة، واختر "خصائص" (Properties)، ثم انقر قسم "تفاصيل" (Details).
وحتى لو بدت ترويسة الرسالة غير مفهومة لك، فيمكنك استخدامها للتأكد إذا كانت جهة حقيقية ردت الرسالة أم لا. راجع السطر To: للتأكد من أنه يحوي عنواناً بريدياً شرعياً، وإذا وجدته، فهذه رسالة رد شرعية تفيد عدم تسليم رسالة من رسائلك صادرة عن المزود الذي أرسلت إليه هذه الرسالة.

البريـــد المـــوثـــق

كيف تتأكد أن رسالة البريد الإلكتروني التي تصلك من والدتك أنها فعلاً منها؟ فالبريد الإلكتروني لا يقدم حالياً أية وسيلة ذاتية للتحقق من الهوية. وتوجد محاولات جارية لإضافة نوع من أنواع التحقق بين مزودات البريد، ولكن خيارات التحقق الشخصية متوفرة منذ سنوات. فوالدتك لا تحتاج إلا إلى شهادتها الرقمية لإثبات نفسها.

اشتر شهادة رقمية

عندما تتلقى رسالة موقعة رقمياً، فإنها تكون مرفقة بأيقونة ختم. انقر على هذه الأيقونة نقراً مزدوجاً، وابدأ في البحث عن مصدر الشهادة، وستعرف معلومات عن المرسل، وربما عن جهة التوثيق أيضاً. وهذه الأخيرة عبارة عن شركة تصدر شهادات (مقابل مبلغ معين عادة) وتضمن المعلومات التي تتضمنها. وللحصول على شهادة في آوتلوك، انقر "أدوات|خيارات" (Tools|Options) وتوجه إلى قسم "أمان" (Security). انقر على الزر "إحضار معرف رقمي" (Get a digital ID..) القريب من نهاية النافذة. وسيتم فتح نافذة متصفح على صفحة على موقع مايكروسوفت تحوي معلومات حول بائعي الشهادات الرقمية.

أو احصل على شهادة مجانية: توجد أدوات يمكنك الحصول عليها مجاناً لإصدار شهادات فريدة، ولكن، إن لم تكن هذه الشهادات مسجلة لدى جهة عامة، فإن كل ما تثبته هو أن الرسائل التي أرفقت بها لم يتم التلاعب بمحتوياتها. وتوجد فكرة أفضل، وتتمثل في القيام بزيارة إلى الموقع www.thawte.com، وهو موقع تابع لشركة VeriSign يعرض شهادات شخصية مجانية.

فائـــدة الشهـــادات

تسمح لك الشهادات الرقمية بتشفير محتويات الرسائل وإثبات عدم حدوث تلاعب بها، ويمكن لبرنامج التخاطب الفوري Instant Messenger من AOL (وتطبيقات أخرى) أن يستخدم شهادتك الرقمية لإثبات هويتك على إنترنت.

استخدام آوتلوك فى التشفير

يمثل المعيار S/MIME (أو الامتدادات الآمنة لبريد إنترنت متعدد الأغراض)، المعيار للبريد المشفر و"الموقع". وكل الإصدارات الحديثة من آوتلوك وآوتلوك إكسبريس ويدورا و Netscape Messenger تدعمه، ولكن لا يوجد برنامج أسهل في التعامل مع الشهادات من آوتلوك.

شــــيء مـــزيـــف

عند البحث عن صفقات على إنترنت، عليك أن تكون متشككا تجاه المواقع التي لا توجد وصلات لها بها والتي لم تسمع عنها من قبل. فالمحتالون يبذلون جهداً كبيراً للحصول على ترتيباً متقدماً في نتائج البحث التي تجريها محركات البحث الشبكية لجذب الباحثين عن الصفقات. والوصلات التي تقود لهذه المواقع والمتاجر المبهمة تؤدي إلى صندوق حوار تحمل غالبا شكل "شيك مصرفي" وتسألك عن اسم بطاقة الائتمان الخاصة بك ورقمها وتاريخ انتهائها، والرقم الخاص CVV (قيمة التحقق من البطاقة). وبعد أن تعطيها المعلومات التي تريدها، يتم توجيهك إلى صفحة تقول إن خطأً قد حدث وأن عليك الدفع عن طريق حوالة بريدية. وهذا يعني أن بعض الضحايا قد يفقدون معلومات بطاقة الائتمان الخاصة بهم، وقيمة الحوالة المالية أيضاً.

لا تكن مركز جذب للرسائل التطفلية

لا يجني مرسلو الرسائل التطفلية أرباحهم من نشر الإعلانات فقط، لكن، من خلال إعادة بيع قوائمهم التي تتضمن عناوين الضحايا البريدية، وكلما زاد عدد الضحايا الموثوق بأنهم "أحياء" في القائمة، كلما ارتفعت قيمتها.

لا للشراء بهذه الطريقة

أسوأ ما يمكنك فعله هو شراء شيء من مروج رسائل تطفلية. فهذا يعني وضعك على قائمة الضحايا "الأحياء" الحقيقيين.

لا لإزالة الاشتراك

لا تنقر زر "إزالة الاشتراك" (Unsubscribe)، أو زر "الإزالة من القائمة" (Remove me from your lists) أو ما شابه ذلك من أزرار ووصلات تجدها في نهاية الرسائل التطفلية. ففعل هذا يثبت لهؤلاء المتطفلين أن عنوانك صحيح. لاحظ أن كثيراً من المواقع الشرعية – مثل e-tailers أيضاً تعرض وصلة لإزالة الاشتراك في نهاية رسائلها البريدية، لكن هذا الموقع محترم.

لا لفتح الرسائل المشبوهة أو معاينتها

يمكن لمرسلي البريد التطفلي التأكد من وجودك عندما تفتح رسالة تطفلية مهيأة بواسطة HTML. فمن خلال الصور الموجودة ضمن هذه الرسالة، أو بعض الثغرات الشبكية، يصل تنبيه إلى المزود الذي يعمل عليه المروج يفيده بأنك فتحت رسالته. وتعالج أحدث إصدارات آوتلوك وآوتلوك إكسبريس ذلك بعدم تحميل الصور حتى تأمرها بذلك. فإذا لم تكن تعلم المرسل، فلا تفتح الصور.

تأمين

التصفح

الشبكي

بينما تسمح لك الإعدادات الافتراضية لإنترنت إكسبلورر بالتمتع بكامل ما تعرضه الشبكة، فإنها أحياناً تكون مفتوحة على المخاطر بشكل غير مقبول. وإليك بعض الوسائل لتضييق الفجوات الأمنية في إنترنت إكسبلورر.

العمل من الداخل

افتح لوحة التحكم، ومنها خيارات إنترنت، للوصول إلى إعدادات إنترنت إكسبلورر. في مربع حوار خصائص إنترنت، اختر قسم "أمان" (Security)، ثم انقر على زر "مستوى مخصص" (Custom Level). ويمكنك التجول عبر مختلف الإعدادات الموجودة هنا. وفي كل منها، يمكنك الاختيار بين ثلاثة أوضاع، إما تمكين الوظيفة، أو إظهار محث بشأنها، أو تعطيلها.

عطـــل افتراضيـــاً

في معظم الحالات، يكون من الأفضل أن تعطل أي شيء مثير للجدل. فإذا اخترت أن يتم سؤالك في كل مرة، فقد تجد الكثير من رسائل التنبيه المزعجة تظهر لك بعكس ما كان يحدث في الماضي.

امنع النوافذ المنبثقة

يعدّ منع الشيفرات النشطة active scripts تماماً من العمل خطوة قاسية، لأن كثيراً من المواقع تستخدم هذه الشيفرات لأغراض شرعية. لكن إن كنت ترتاد مواقع تظهر بها نوافذ منبثقة كثيرة لا ترغب بها، جرب هذه الطريقة: تجول في قائمة "إعدادات الأمان" (Security Settings) في إنترنت إكسبلورر حتى تصل إلى البند: الشيفرات Scripting، وعطل كل الإعدادات (وعددها ثلاثة في إنترنت إكسبلورر 6). كما قد ترغب أيضا في تعطيل أدوات التحكم ActiveX، فلا ننصح بتمكينها تلقائياً. ويمكنك حظر أدوات التحكم الموقعة (التي تتمتع بشهادة رقمية صالحة) أو غير الموقعة. أما في وضع الأمن المتوسط Medium، فيتم تعطيل أدوات التحكم غير الموقعة، بينما يسمح بظهور الموقعة منها.

أقـــــم الثــقـــة

ماذا لو رغبت في تعطيل الشيفرات مع معظم الصفحات، ولكن مع إتاحة الاطلاع على موقع eBay (وهو يعتمد الشيفرات بكثرة) بدون أن تظهر رسائل التنبيه الكثيرة؟ الحل يكمن في الإعدادات التي يحويها إنترنت إكسبلورر والتي تسمح لك بالتعامل مع هذه المواقع "الموثوق بها" (trusted) بدون الإخلال بقواعد الأمن العامة. ولإضافة المواقع التي تكثر من زيارتها في فئة المواقع الموثوق بها، اختر "أدوات"، ثم "خيارات إنترنت" وانقر على لسان تبويب "الأمان" (Security). سترى الآن عدة أيقونات خاصة بما يعرف بـ"مناطق المحتوى الشبكي" (Web content zones)". انقر على الأيقونة الخاصة بالمنطقة "مواقع موثوق بها" (Trusted sites) ، ثم انقر على زر "مواقع" (Sites). اكتب اسم النطاق الخاص بالموقع الموثوق به، مثل eBay.com وانقر على "إضافة" (Add)، وقد تحتاج لإزالة العلامة الموضوعة أمام الخيار "مطلوب تحقق الملقم (https:) لكافة المواقع في هذه المنطقة" (Require Server Verification (https:) for all sited in this zone).
وسوف يضيف إنترنت إكسبلورر العلامة "*" قبل اسم نطاق الموقع، على الرغم من أنك لن تراها إلا إذا خرجت ثم أعدت الدخول إلى صندوق الخصائص. وبعدما تنتهي، انقر على "موافق" (OK). وتتمتع منطقة المواقع الموثوقة بمستوى أمني منخفض Low-Level، يسمح بتنزيل محتوى مثل أدوات تحكم أكتيف إكس، والبرامج المضافة Plug-ins، وملفات الارتباط (الكوكيز)، وكل أنواع الشيفرات المماثلة. ولكن، سيظل البرنامج يمنع وصول أدوات تحكم أكتيف إكس غير الموقعة.
لماذا نتلقى رسائل تحذير حتى الآن؟ إذا كنت قد ضبطت خيار تنزيل الشيفرات وأدوات تحكم أكتيف إكس على Prompt ليتم سؤالك عن كل منها، فقد تستمر في تلقى تحذيرات خاصة بها على المواقع الموثوق بها. وهذا يرجع إلى أن هذا الموقع الموثوق به يدعم في العادة الإعلانات التي تستضيفها مواقع أخرى غير موثوق بها.

كن مختلفاً وبدل برنامج التصفح

يبحث معظم الفيروسات والديدان ومصممو برامج التجسس عن أكبر عدد من المستهدفين. وهذا هو السبب الرئيس في أنهم يهاجمون ويندوز وإنترنت إكسبلورر خاصة. ومن أيسر الخطوات لتقليل المخاطر التي قد تتعرض لها أن تنتقل إلى المتصفح المجاني فاير فوكس، أو إلى أوبرا (والذي يخلو من الإعلانات أيضا الآن). ومع هذا لا يمكن أن نعتبر الانتقال إلى متصفح أقل شعبية حلاً سحرياً، ولذا، عليك أن تحافظ على إعداداتك الأمنية في الوقت ذاته.

بدل نظام التشغيل !

توجد خطوة أكثر حسماً، ولكن لن تكون سهلة على بعض المستخدمين ولكن لا بأس من أخذها في الاعتبار، وهي الانتقال من منصة الحاسوب الشخصي تماماً وشراء جهاز من نوع ماكنتوش، أو استخدام نظام التشغيل لينكس المجاني والمفتوح المصدر، والذي يعمل على معظم الأجهزة المتوفرة حالياً. وتوجد أسئلة مثارة بالفعل عن إذا كانت شيفرة هذه المنتجات "غير المايكروسوفتية" أكثر أمناً، ولكن، لمجرد أنها أبعد عن أن تلحظها أعين المتربصين، تقل احتمالات استهدافها.

تغيير شكل البرنامج لديك

من بين الأساليب الشائعة التي تعتمدها الهجمات الزائفة إدخال تغييرات على عنوان URL المعروض في سطر العنوان في برنامج إنترنت إكسبلورر من خلال إظهار نافذة صغيرة فوقه تتضمن العنوان الزائف.

ومن بين أسباب نجاح هذه الطريقة أن سطر العنوان له في العادة مكان افتراضي ثابت. فإذا نقلته، ستظهر النافذة المنبثقة مرة أخرى، ولكن، سيتضح أنها عنوان زائف، لأنها تظهر في غير الموضع الذي اعتادت الظهور فيه.

حرك الأســـــطر

يمكنك نقل أي من أسطر العناوين والقوائم في إنترنت إكسبلورر بالنقر على سطر النقاط الرأسي الموجود عند الطرف الأيسر من هذه الأسطر مع سحبه. وإذا صادفت مشكلات في نقل هذه الأسطر، فقد يكون السبب هو أنها مثبتة Locked في موضعها. انقر بالزر الأيمن على مساحة خالية على أي من أسطر الأدوات، وأزل العلامة الموضوعة أمام الخيار Lock the Toolbars لإزالة هذا التثبيت.

لا تسمح بالسطو على متصفحك

غدا السطو على المتصفح Hijacking أحد أكثر المشكلات التي تواجه المستخدمين في المنزل، وفي مكان العمل شيوعاً. فأنت تبحر إلى أحد المواقع، وفجأة، تجد أن متصفحك يصر على فتح موقع بحث معين، وأن الصفحة الرئيسة للمتصفح تغيرت. بل، وتجد أن المحتالين المسئولين عن ذلك يتابعون نتائج إعلاناتهم الموجهة (على شكل نوافذ منبثقة عادة) في متصفحك.
ومعظم هذه الصفحات المثيرة للتبرم تروج في الغالب لخدمة أو منتج معين، ولكن بعض الهجمات تكون مرفقة ببرامج من نوع أحصنة طروادة، أو من نوع "الأبواب الخلفية" (backdoors) وتسمح للمنتفعين بتنزيل تحديثات، وجمع معلومات عن الضغطات التي بها على لوحة المفاتيح وغيرها من البيانات.

التزم جانب التشكك

تصل معظم هجمات الهكرة من خلال تفاعل المستخدم. فإن ظهرت أمامك نافذة منبثقة تطلب تنزيل أداة عرض viewer معينة، أو تنزيل برنامج مجاني، أو تطلب، في أبسط صورها، تغيير صفحتك الرئيسة، فانقر على No أو أغلق هذه النافذة.
احصل على التحديثات باستمرار: تأكد من توفر جميع تحديثات ويندوز وتحديثات برامج مكافحة الفيروسات لديك. فمعظمها يمكنه وقف هجمات الهكرة عند الباب الأمامي.

نظــف حاسوبـــك

إن وقعت ضحية لهجمة هاكر، استخدم برنامجا لمكافحة التجسس لفحص حاسوبك (مثل البرامج المجانية Microsoft Antispyware beta وSpy Catcher Express أو Ad-Aware أوSpybot Search &Destroy) لإزالة الشفرة الخبيثة تماماً.

الأمـــن

من البرامـــج

الخبيــــــــــــــــــــــــــثة

تغيير برامج مكافحة الفيروسات

تتيح معظم منتجات مكافحة الفيروسات تنزيل تحديثات لها لمدة عام كامل بدءا من تاريخ فتح علبة المنتج، مع إتاحة خيار الحصول على تحديثات لمدة أطول في مقابل مادي. ولكن، أحيانا قد تحتاج إلى الانتقال إلى منتج جديد تماما، إما من نفس الشركة، أو من غيرها. وتذكر، أن منتجات مكافحة الفيروسات لا تتعايش معا بالشكل المطلوب. وحتى لو لم يعد أحدها حديثاً، فإن ضبط بحيث يفحص الملفات لدى استخدامها، فإن هذا يعني أنه "يراقب" عمليات الاتصال بإنترنت، كما يراقب استخدام الملفات. وكثير من هذه البرامج يستخدم أيضا مزودا وكيلاً Proxy للبريد الإلكتروني يعيد توجيه البريد الوارد والصادر ليمر من خلال أداة فحص، وهذا كله قد يتعارض مع منتجات مكافحة الفيروسات الجديدة، أو قد يعيق أداءها، على الأقل.

وداعــاً للقــديم

ألغ تثبيت برنامج مكافحة الفيروسات القديمة لديك وأزلها قبل تثبيت البرنامج الجديد. فإن كان البرنامج القديم محدثاً بما يكفي، قم بعملية فحص نهائية لحاسوبك باستخدامه قبل إزالة تثبيته للتأكد من أنك ستبدأ نظيفاً مع البرنامج الجديدة. ومن الضروري بصفة خاصة أن يكون برنامج جدار النار لديك (أو حتى برنامج Windows Firewall) نشطاً خلال الفترة الزمنية التي تفصل بين قيامك بإزالة البرنامج القديم وتثبيت آخر جديد.

في تلك الأثناء

إذا انقضى أكثر من أسبوع منذ تحديث برنامجك القديم لآخر مرة، استخدم برنامجاً شبكياً لفحص الحاسوب، مثل برنامج HouseCall المجاني من شركة Trend Micro، أو أداة Stinger من مكافي، أو ActiveScan من Panda Software (طالع قائمة الأدوات والمواقع المرفقة لمعرفة المزيد من الأدوات). وقبل أن تزيل البرنامج القديم، أغلق كافة الصفحات الشبكية المفتوحة أمامك، وكذلك أغلق برنامج البريد الإلكتروني لتقليل مخاطر التعرض لهجمات.

عطل الخدمة أولاً

قد تحصل على تحذير يطالبك بتعطيل برنامج مكافحة الفيروسات القديم قبل إزالته، وهو ما يمكنك القيام به مع معظم المنتجات من خلال النقر بالزر الأيمن على أيقونته الموجودة في صينية النظام (قرب الساعة القابعة في الجزء السفلي من الشاشة). فإن سألك البرنامج عما إذا كنت تريد حذف محتويات مجلد الحجر المؤقت Quarantine أو مجلد الملفات التي تم نسخها احتياطياً، فانقر على نعم، حيث سيعثر عليها البرنامج الجديد بعد تركيبه على الأرجح.

بدء العمل بالبرنامج الجديد

تثبت البرنامج الجديد، وحدث ملفات التعريف الخاصة به على الفور. وبعد ذلك، أجر فحصاً شاملا لحاسوبك. وأخيراً، تأكد من تمكين وظيفة الفحص لدى الاستخدام.

زيف وإزعـــاج

ماذا تفعل عندما تظهر أمامك نافذة تحذير منبثقة تفيد بأنك تعاني من مشكلة أمنية؟ اعلم أن المحتالين يحاولون استغلال عصبية بعض المستخدمين، بإظهار ما يبدو وكأنه تحذير من برنامج أمني، فالنقر في أي مكان في مثل هذا الإعلان، سواء على أي من زري Yes أو No، أو في أي مكان آخر، قد يأخذك إلى الموقع الشبكي الخاص بهؤلاء المحتالين، حيث يتم تنزيل برامجهم. ونصيحتنا هي: تجاهل هذه الرسائل وأغلق نوافذها فوراً باستخدام مفتاحي Alt + F4.

إزالة القناع عن الدجالين

قد تبدو هذه النوافذ المنبثقة شديدة الشبه بمربعات حوار ويندوز وأحيانا بقوائمها أيضاً. فكيف تعرف ما إذا كانت إعلاناً أم لا؟
حتى إذا كان ويندوز يعرض عليك رسالة ملحة، فلا تقلق ولا تنزعج، واحتفظ بهدوئك. فإن نظرت إلى سطر العنوان وسطر الحالة، في أعلى وأسفل النافذة، يمكنك أن تتأكد مما إذا كانت هذه النافذة نافذة إنترنت إكسبلورر. وهذا دليل يساعدك، ولكنه ليس دليلاً قاطعاً على أن هذه النافذة ليست تحذيراً أمنياً.

ولكـن، إن كنـت لا تـزال فـضولياً، انقـر بـالزر الأيمـن علـى النافـذة، واختـر خـصائص Properties. وستعرف الموقع الذي ظهرت منه. فأي مربع حوار حقيقي من ويندوز يعتمد برنـامج إنترنت إكسبلورر سيكون لـه عنـوان غيـر تقليـدي يبـدأ بحـروف غيـر تقليديـة، مثـل الحروف res:. أما الإعلان الشبكي، فسيكون له عنوان موقع عادي.

أدوات مكافحة التجسس ووداعاً للنوافذ المنبثقة

تتيح المواقع جوجل وياهو وإم إس إن أدوات مجانية لمنع ظهور النوافذ المزعجـة. ويتـضمن المتصفحين أوبـرا وفـاير فـوكس أدوات مماثلـة مبيتـة، كمـا تـضيف الإصـدارة الخدميـة الثالثـة لويندوز إكس بي أداة مماثلة إلى إنترنت إكسبلورر. فضلاً عن ذلك، زُودت كثير من بـرامج مكافحة الفيروسات بـأدوات لمنـع ظهـور هـذا النـوع من النوافذ، لـذا، لا حاجـة لـشراء أدوات خاصة. لكن عليك استخدام أداة من شركة تثق بها.

التهديدات الأعنف

تـروج بعـض بـرامج مكافحـة التجـسس المغمـورة أو المـشتبه بهـا لنفـسها مـن خـلال النوافـذ المزعجة نفسها التي تدعي أنها تزيلها، بل، وترهق المستخدم بتكتيكات ضاغطة كثيرة.
ومن أبرز سمات هذه المنتجـات أنهـا مجانيـة التنزيـل والفحص، لكـن إن رغبـت فـي تنظيـف حاسوبك باستخدامها، تجبرك على شراء رخصة استخدام. وبعضها يظهر رسائل خادعة تفيد بوجـود بـرامج تجـسس لـديك لتقنعـك أكثـر بـشرائها. وأكثرهـا خباثـة، ويطلـق عليـه بـرامج "مبتـزة"، تـستخدم بـرامج تركيـب خبيثـة، وتعيـق محـاولات إلغـاء التركيـب، وأحيانـاً تـسبب مشكلات في الاتـصال بإنترنـت، إلا إذا اشـتريتها. وبعـض هـذه المنتجـات هـي بالفعل بـرامج تجسس، تسجل بيانات عنك، وترسلها إلى مواقع الجهات المصممة لها.

كيف تعرف الفرق ؟

كقاعدة عامة، إن استخدم البائع إعلاناً منبثقا للإعلان عن أنه يخلص حاسوبك من النوافذ المنبثقة وبرامج التجسس، فعليك أن تعتبره مشتبها به. وعلى الرغم من أن بعض برامج مكافحة التجسس التجارية الجيدة تتيح عمليات فحص مجانية، فإن الشرعية منها لن تنص في إعلان عن أنها اكتشفت لديك حالة إصابة.

احصل على المساعدة

يقدم الموقع SpywareWarrior.com قائمة بأكثر من 90 برنامجا تم التأكد، أو الاشتباه، في كونها ذات طبيعة غير معروفة أو مريبة وذلك كوسيلة لحمايتك من برامج التجسس. وأيضا يمكنك مراجعة الموقع www.spywareguide.com (SpywareGuide) الذي يتيح الكثير من المعلومات والتلميحات بهذا الشأن.

اقرأ النشرات والاتفاقيات

يتطلب الاحتفاظ بحاسوبك نظيفاً من برامج التجسس، والإعلانات، والبرامج الخبيثة، مثابرة ووعياً من جانبك. انتبه لطلبات تنزيل البرامج على حاسوبك. فلا توافق على أي شيء إلا إذا قمت بقراءة اتفاقية الاستخدام. وإن بدا شيء معين مخادعاً، فأغلق برنامج التصفح.

هنـــا مضيفـــك

عندما تكتب اسم موقع معين، مثل (www.kutub.info)، (وهو موقعنا المفضل الذى يزودنا بالمعلومات والنافذة التى نبث منها الكتب) فإن المتصفح يتصل بمزود أسماء نطاقات DNS مركزي بالبحث عن الموقع، ويترجم هذا العنوان الذي كتبته إلى عنوان IP رقمي. ولكن لكل نسخة من نظام التشغيل ويندوز مزود نطاقات مصغر يسمى ملف المضيف hosts، وهو ملف يطالعه المتصفح أولاً قبل الاتصال بالمزود المركزي الخارجي على الشبكة.

أصبح هذا الملف هدفاً محبباً للفيروسات وبرامج التجسس وأدوات السطو على المتصفحات، والتي يمكنها استخدامه لتوجيه كل طلبات فتح المواقع المختلفة، مثل ياهو وجوجل، إلى صفحة البحث الخاصة بها من خلال وضع أسماء هذه العناوين مع الإشارة إلى عنوان IP

معين واحد. وتستخدم بعض الفيروسات والديدان هذا الملف لمنع الاتصال بمواقع مكافحة الفيروسات أيضاً، وتوجهك، بدلا من ذلك، إلى نظامك الخاص، ممثلا بعنوان IP المحلي 127.0.0.1.
ويعد إصلاح ملف hosts عملية سهلة- فما عليك سوى تعديله ببرنامج الدفتر Notepad. وستجده بصفة عامة في مجلد ويندوز. فعلى نظام ويندوز إكس بي، ستجده على المسار: C:\Windows\System32\Drivers\Etc وعلى نظام ويندوز 2000، ستجده في المسار: C:\Winnt\System32\Drivers\Etc.

وفي هذا الملف، تعتبر الأسطر التي تبدأ بعلامة # تعليقات لا تؤثر بشيء، لذا، فالسطر النشط الوحيد هو السطر الأخير الذي يوجه المضيف المحلي إلى العنوان 127.0.0.1.
وقد يتضمن ملف مضيف تم السطو عليه أسطرا تشبه التالي:

msn.com 66.250.107.100
www.msn.com 66.250.107.100
search.msn.com 66.250.107.100
auto.search.msn.com 66.250.107.100

وهذا يعني أن أية محاولة للوصول إلى موقع MSN، ستؤدي إلى فتح هذه الصفحة البديلة التي يشير إليها رقم IP الموضوع أمامها. كما قد يبدو بهذا الشكل:

localhost 127.0.0.1
liveupdate.symantec.com 127.0.0.1
update.symantec.com 127.0.0.1
download.mcafee.com 127.0.0.1
www.symantec.com 127.0.0.1
www.sophos.com 127.0.0.1

وهذا يعني أنك ستحصل على رسالة خطأ كلما حاولت الوصول إلى مواقع مكافحة الفيروسات المذكورة.
ولإصلاح هذا الملف، يمكنك حذف كل الأسطر الموجودة فيه ما عدا السطر الذي يحدد المضيف المحلي. فإن لم تجد هذا السطر، أنشئ ملفا نصياً بسيطاً لا يتضمن سواه، أي لا يتضمن سوى السطر localhost 127.0.0.1، واحفظه باسم الملف hosts (بلا امتداد) على المجلد عينه.
لاحظ أنه يمكنك أيضاً استخدام ملف المضيف لمنع فتح المواقع غير المرغوب فيها، من خلال إضافة عناوين هذه المواقع إلى هذا الملف وإعادة توجيهها إلى المضيف المحلي.

التعرف على اوجه الشقاوة

كثير من البرامج الخبيثة، وحتى ذات الأغراض الحميدة منها، تضيف مواداً غير مرغوب بها إلى مجلد بدء التشغيل. ويعد ملء الذاكرة أحد الأسباب الرئيسة وراء تباطؤ عملية تحميل الحواسيب، وأيضا تباطؤ عملية التشغيل، وعدم استقرار النظام بصفة عامة. فكلما زاد عدد الأشياء التي يتم تحميلها أثناء بدء الحاسوب، كلما تباطأت عملية التحميل، وكلما قلت بعد ذلك المساحة المتاحة في الذاكرة لتشغيل البرامج الأخرى.

شغل برنامج MSconfig: تسمح لك أداة تهيئة النظام Msconfig بتعديل البرامج التي يقوم ويندوز بتحميلها عند بدء التشغيل. انقر "ابدأ" (Start) ثم "تشغيل" (Run) واكتب msconfig، واضغط زر الإدخال. استخدم قسم "بدء التشغيل" (Startup) لتمكين/ تعطيل ملفات بدء تشغيل بعينها. ويمكن أن تلجأ لتعطيل كافة الملفات هنا لمعرفة المشكلات التي يعاني منها حاسوبك. وفي معظم الحالات، يتيح تعطيل كافة عناصر بدء التشغيل بإقلاع ويندوز بشكل نظيف، ويمكنك بعدها البدء بإعادة إضافة الملفات التي تريدها، مثل واجهة المستخدم الخاصة ببرامج مكافحة الفيروسات وجدر النار التي تعمل عند الإقلاع. ملحوظة مهمة: إن كنت تستخدم Msconfig، تأكد من عدم إدخال أية تعديلات في قسم Services.

التعرف على الملفات الخبيثة

كيف يمكنك أن تعرف أي ملفات بدء التشغيل جيد يجدر الاحتفاظ به، وأيها ليس كذلك؟ يمكنك أحياناً أن تحصل على فكرة عن ماهية ملف معين بالنظر إلى العمود Command أو Location المجاور لاسمه في قسم Statup في برنامج Msconfig. فالأمر Command هو اسم الملف التنفيذي، وسطر الأمر الذي يستخدم لتشغيل هذا الملف. وأما الموضع Location، فيوضح من أين تم تشغيل هذا الملف، وفي العادة يكون من مفتاح في سجل النظام Registry، أو من مجلد بدء التشغيل في ويندوز.

فإن لم تفلح هذه الطريقة في مساعدتك على تحديد الملفات المطلوبة من غيرها، قم بزيارة الموقع www.sysinfo.org وراجع قاعدة بياناته لتحديد ما إذا كان أي ملف من هذه الملفات مطلوب أو مرتبط بالنظام، أو بالتطبيقات الأخرى، أو بشيفرات خبيثة.

كما يمكنك البحث عن اسم الملف المشتبه به على موقع البحث جوجل. والنتائج غالبا ما تشمل تعريفا من مواقع مثل: AnswersThatWork.com أو WinTasks Process (www.liutilities.com/products/wintaskspro/processlibrar Library) كما يمكن للبرنامج WinTasks أن يساعدك في تصنيف العمليات processes التي تظهر في مدير المهام في ويندوز. وبعد التعرف على هوية الملف، يمكنك تمكينه أو تعطيله. وعندما تنتهي، انقر على OK (أو Apply ثم OK). وسوف يسألك ويندوز عما إذا كنت تريد إعادة

تحميل الحاسوب، ثم يعرض عليك رسالة تحذير تخبرك بأنك تستخدم وضع التحميل الاختياري. ويؤدي النقر على Ok في هذه الرسالة إلى تشغيل برنامج Msconfig مرة أخرى. ويمكنك تجنب هذا بالضغط على خيار Don't show this again.

التقاط البقايا المتناثرة

لا تتمكن أدوات إزالة برامج التجسس من تنظيف كل العوالق الباقية بعد حذف هذه البرامج دائماً.

لا للقلـــق

القضية الأساسية هي إذا كان أي من هذه العوالق المتروكة قادراً على أن يعمل أم لا، وفي الغالب، لن تجدها تعمل. ولكن، بالنسبة لمن يحبون العمل على نظام نظيف تماما، يمكن لأداة إزالة برامج التجسس أن تضعك على الطريق الذي يمكنك بعده البحث يدويا عن أية عوالق وإزالتها. وستجد الأمر أسهل إن كانت هذه البقايا مخزنة في مفاتيح سجلات أو مجلدات معرفة بأسماء معبرة، ولكن، إن كان البرنامج يختفي في مجلد نظام التشغيل ويندوز، فيصبح التعرف عليه أصعب.

أجر فحصاً ثانياً

افحص حاسوبك باستخدام برنامج آخر. فهذه العملية الثانية قد تعتبر وجود هذه العوالق دليلاً على أن البرامج الخبيثة لم تذهب، ومن ثم تساعدك على تحديد موضعها وإزالتها. وطالما كنت متنبها لتشغيل برنامج فحص واحد في وقت واحد، فلن تعاني من أية تعارضات بين هذه البرامج المتشابهة في وظائفها.

تأمـــين

الأجهـــــــزة

النقـــــــــــالة

ابق حذراً عند الاتصال بالبقع الساخنة

تصفح إنترنت أثناء جلوسك في المقهى المجاور لك شيء عظيم، ولكن الشخص الذي يجلس على بعد عدة مقاعد منك قد يتصفح معك حاسوبك المفكرة أيضاً، وقد يحمل بيانات شخصية أو بيانات خاصة بشركتك. فغالباً ما تتيح مواقع الاتصال اللاسلكي الساخنة بإنترنت لمخترقي النظم حفظ بياناتك واستعادتها بسهولة نسبية. ولذا، عليك فعل شيئين:

الأول عطل وظيفة مشاركة الملفات:

في ويندوز إكس بي، افتح لوحة التحكم، ومنها اختر "اتصالات شبكة الاتصال" (Network Connections). انقر بالزر الأيمن على البطاقة اللاسلكية، واختر خصائص. وفي قسم "عام" (General) في صندوق الحوار الذي يظهر، انتقل خلال قائمة العناصر التي تستخدمها البطاقة، وأزل العلامة الموضوعة أمام الخيار File and Printer Sharing for Microsoft Networks.

الشيء الثاني استخدم جدارا ناريا شخصيا:

استخدم منتجا يدعم المناطق الأمنية، مثل Norton Personal Firewall وسيشعر الجدار بأنك على شبكة جديدة، وسيسألك إن كنت تثق بها أم لا، فاختر لا.

أمن الحواسيب العمومية

وجود الحواسيب العمومية في مقاهي إنترنت والمكتبات والمطارات شيء طيب ومفيد، ولكنها تتطلب يقظة عالية.

انظـــر إلى ما حولـــك

تأكد أن أحداً لا يستطيع أن يلقي ببصره على شاشتك أو لوحة مفاتيحك.

احذر برامج تسجيل ضغطات المفاتيح

كثير من الحواسيب العامة أعدت بحيث لا تسمح بتنزيل أية برامج إضافية إليها إلا بموافقة المدير. ولكن، يوجد احتمال أن يتمكن أحد الهكرة من تركيب أحد أحصنة طروادة من نوع البرامج التي تسجل ضغطات المفاتيح لتسجيل ضغطاتك، بل إن بعض المخترقين الأكثر إصراراً وحنكة قد يتمكنون من استخدام أداة خاصة – مثل الأداة KeyGhost HardwareKeyLogger تصل بين لوحة المفاتيح والحاسب الشخصي. وقد يظن البعض

للوهلة الأولى أن هذه الأداة جزء طبيعي من كبل لوحة المفاتيح. فإن أمكنك، افحص موضع اتصال لوحة المفاتيح بمؤخرة الحاسوب للتأكد من عدم وجود توصيلات إضافية. فإن وجدت أيا منها، ابحث عن حاسوب آخر. وتوجد حيلة أخرى ماكرة هي أن تضغط "ابدأ|البرامج الملحقة|الوصول|لوحة مفاتيح على الشاشة" (Start|Accessories|Accessibility|On Screen Keyboard) وتكتب كلمات السر التي تريدها باستخدام الماوس، كما يمكنك أن تكتب كلمة السر بلوحة المفاتيح العادية، مع وضع حروف غير صحيحة في المنتصف، ثم استخدم الماوس لحذف هذه الأحرف الدخيلة.

لا تعض يـــدك ندمـــاً

ننصح بتجنب كتابة أية بيانات مهمة على الحواسيب العامة. وأيضاً، لا تبتعد كثيراً عن الحاسوب بعد أن تسجل دخولك عليه. فكثير من المواقع (مثل eBay) تضع ملفات ارتباط (كوكيز) خاصة بكل جلسة شبكية، وهكذا، لن تضطر لتسجيل الدخول إليها مرة أخرى إن أغلقت المتصفح ثم أعدت فتحه. فإن أغلقت المتصفح، وسرت بعيداً، فقد يتمكن المستخدم الذي يليك من المواصلة من حيث انتهيت. كما يمكن لحسابات Microsoft Passport وياهوو أن تظل موجودة على الحاسوب. فإن وجد النظام ويندوز إكس بي على الحاسوب العمومي، فقد يسألك عما إذا كنت تريد ربط حساب Passport الخاص بك بحساب ويندوز إكس بي، فتأكد من اختيار لا.

امـــح آثـــــارك

تأكد من حذف كل آثارك الإلكترونية على الحواسيب العمومية من ملفات مؤقتة، وملفات ارتباط (كوكيز)، وملفات سابقة history. فإن كنت تستخدم إنترنت إكسبلورر، فانقر "أدوات|خيارات إنترنت" (Tools|Internet Options). وفي قسم "عام" (General)، انقر على "حذف ملفات تعريف الارتباط" (Delete Cookies)، وانقر أيضاً على حذف الملفات التصفح المؤقتة "حذف ملفات" (Delete Files) (وتأكد من وضع علامة أمام الخيار "حذف كافة المحتويات دون اتصال" (Offline Content)، واحذف أيضاً ملفات التصفح السابقة بالنقر على "مسح المحفوظات" (Clear History).
وأنت لا تزال في نافذة خيارات إنترنت، انقر على لسان التبويب "محتوى" (Content)، ثم انقر على زر "إكمال تلقائي" (AutoComplete). وفي صندوق الحوار الذي سيظهر، انقر على زر "مسح النماذج" (Clear Forms)، وعلى زر "مسح كلمات المرور" (Clear Passwords).
إن قمت بتنزيل أية وثائق، احذفها أيضاً. وإن حررت أية وثائق، قم بحذفها من قائمة "الوثائق الحديثة". وللقيام بذلك في ويندوز إكس بي، انقر بالزر الأيمن على سطر المهام أسفل

الشاشة، واختر خصائص. اختر لسان التبويب "القائمة ابدأ" (Start Menu)، وانقر على "تخصيص|خيارات متقدمة" (Customize|Advanced). والآن، انقر على زر "مسح القائمة" (Clear List) الخاص بالمستندات الأخيرة (Recent Documents). وأخيراً، أفرغ سلة المهملات للتخلص تماماً من أية ملفات تم حذفها.

احمل برامجك الأمنية معك

لحماية نفسك بشكل أفضل عند استخدام حاسبات غير حاسوبك، خاصة الحواسيب العمومية، احمل معك ذاكرة من نوع USB محملا ببرامج الحماية النقالة.

استخدم مديرا لكلمات السر

يسمح لك برنامج Pass2Go من شركة Siber Systems (www.pass2go.com)، مثلاً، بتخزين جميع كلمات سرك على إصبع ذاكرة USB، ويملأ جميع استمارات الدخول في برنامجي إنترنت إكسبلورر وفاير فوكس تلقائياً، ويجنبك المخاطر التي تمثلها برامج تسجيل ضغطات المفاتيح. ويمكن تشفير كل البيانات بكلمة سر رئيسة، وحتى لو تمكن أحد برامج تسجيل الضغطات من التقاط هذه الكلمة، فلا جدوى لها بدون إصبع الذاكرة عينه.

أجر فحصاً قبل الإبحار

توجد برامج لمكافحة الفيروسات وجدر نار تعمل من أصابع الذاكرة ويمكنها أن تتأكد من كون النظام نظيفاً قبل أن تستخدمه. فتأكد فقط من تحديث تعريفات الفيروسات على هذه الأدوات قبل استخدامها في عمليات الفحص.

احتفظ بتطبيقاتك لنفسك

توجد نسخ ذاتية من بعض التطبيقات، مثل فاير فكوس وOpenOffice.org، بتعديل المبرمج جون هولر (www.johnhaller.org)، تسمح لك بالإبحار في إنترنت وتحرير وثائقك بدون لمس متصفح إنترنت أو حزمة الأوفيس الموجودة على الحاسوب المضيف. كما يتيح لك برنامج P.I. Protector Mobility Suite 3.0
الاحتفاظ ببريدك الإلكتروني على إصبع USB، كما يتم الاحتفاظ بكل ملفاتك المؤقتة على هذا المشغل، طالما ظل البرنامج يعمل. وعندما تغلقه، وتجذب المشغل بعيدا عن الحاسوب،

لا تبقى أيـــة آثـــار

لا تبقى أية آثار. كما أن السلسلة الجديدة من المشغلات من النوع U3 Smart Drive تجعل تشغيل تطبيقات مثل هذه أسهل.

اعمل بنظام التشغيل الخاص بك

لاحظ أن بعض التطبيقات النقالة تنشئ ملفات مؤقتة على القرص الصلب الخاص بالنظام المضيف بالفعل. فإن تعطل أحد هذه التطبيقات، فإنه يوجد احتمال أن تبقى بعض آثاره من دون إزالتها تماماً بشكل مناسب. ولحماية أفضل، تتوفر إصدارات من نظام التشغيل لينكس يمكنها العمل على مشغلات USB، كما أن التوزيع Knoppix من هذا النظام يمكنه العمل من قرص مدمج. وإن أمكنك تحميل الحاسوب بهذا المشغل، فأية برامج خبيثة توجد على القرص الصلب لن تستطيع رؤية بياناتك إطلاقاً.

كلمات السر القوية

لا يحمي معظم الحواسيب والكثير من البيانات الشخصية، مثل سجلات البنوك وخدمات الاتصال بالبريد الشبكي، سوى اسم مستخدم وكلمة مرور. أما أسماء المستخدمين، فيسهل تخمينها، بل، وتجدها وقد كتبت مسبقا أيضاً، لذا، فإنك بحاجة إلى التأكد من اختيار كلمات سر قوية – لا يسهل تخمينها أو التعرف عليها باستخدام برامج كسر الحماية التي تعتمد على "القواميس" والتي تطرح ملايين التراكيب الحرفية على مربعات الحوار حتى تصل إلى التركيبة الصحيحة. وتتوفر لدى الكثير من فيروسات إنترنت الأكثر انتشارا قواميس مبيتة تحوي أكثر كلمات السر شيوعاً، وبمجرد وجودها على حاسوبك، يمكنها مهاجمته ومهاجمة غيره من الحواسيب المتصلة به.

إليك بعض النصائح حيال كلمات المرور واسم المستخدم

- لا تستخدم أي جزء من اسم المستخدم في كلمة السر، ولا اسمك الكامل، ولا عنوانك، ولا تاريخ ميلادك، وغير ذلك من المعلومات الشخصية. فهذه البيانات متاحة بسهولة وجاهزة للمقتحمين.
- لا تستخدم كلمات إنجليزية ولا حتى أجنبية.
- تأكد من أن كلمة المرور مكونة مما يتراوح بين ستة وثمانية حروف على الأقل طولا. وكلما طالت كلمة المرور، كلما كان هذا أفضل.
- استخدم أنواعاً مختلفة من الحروف في كلمة مرورك. فعلى الأقل، يجب أن تحتوي كلمة السر على حروف استهلالية كبيرة، وأحرف صغيرة، وأرقام. وإن شعرت بالارتياح لاستخدام الرموز غير الهجائية (مثل # و @ و &) أو حروف آسكي الممتدة (والتي يمكنك استخدامها بالاستمرار في الضغط على Alt أثناء الكتابة على لوحة المفاتيح)، استخدمها.
- غيّر كلمات السر كل فترة تتراوح بين شهر وستة أسابيع.
- لا تكتب كلمات السر على مدونة وتلصقها على الشاشة.
- إن احتجت للاحتفاظ بمستودع لكلمات السر، استخدم برنامجا مثل RoboFormPro (www.roboform.com) الذي يحتفظ بقائمة مشفرة تحوي كل كلمات السر الخاصة بك بكلمة سر واحدة رئيسة. وهذه البرامج يمكنها تزويدك أيضا بكلمات سر قوية حسب مواصفاتك.
- لا تكرر استخدام كلمات السر القديمة ولا تستخدم الكلمة عينها في تطبيقات متعددة.
- استخدم كلمة تعرفها، ولكن، استعض عن الحروف بعلامات الترقيم والأرقام. مثلا، كلمة coffee يمكن أن تصبح COFF33 والاسم MostafaDigital قد يصبح Most@af0aD*ig#it&al2.
- استخدم العبارات في تكوين كلمات السر – أي مجموعة كلمات، بدلا من كلمة واحدة. فإن كنت أحد المعجبين بفريق (الأهلى المصرى) مثلا، فقد تكون العبارة التالية مناسبة تماما: It's not a big motorcycle, just a groovy little motorbike (للترويغ).

لاحظ أن نظم الأمن لا تسمح جميعها باستخدام كلمات سر بهذا الطول، ولا حتى بكلمات سر تحوي فراغات. فمثلاً بعض مواقع التجارة الإلكترونية يسمح لك بما يتراوح بين 8-12 حرف هجاء فقط في كلمة السر. ولكن، منذ طرح ويندوز 2000، والنظام يسمح باستخدام عبارات تصل عدد حروفها إلى 127 ككلمات مرور.

موارد شبكية للتخلص من البرامج الخبيثة

إنترنت مكان يعج بالمخاطر والتهديدات، ولكنه مأوى أيضاً لمئات المواقع المفيدة، والبرامج المجانية، والمتطوعين الحقيقيين الذين يساعدونك في فحص حاسوبك والتعرف على الشيفرات الخبيثة والتخلص منها.

مواقع مفيدة:

• الموقع www.merijn.org) HijackThis): يقدم أداة فحص مجانية للبحث عن برامج التجسس، ويمكنك تقديم ملفات السجل الناتجة عنه إلى الموقع www.spywarewarrior.com أو إلى شركة SpywareInfo (spywareinfo.com)، وسيعمل الخبراء اللطفاء هناك بمعاينة هذه الملفات وإعطائك توجيهات مفصلة وفردية لتنظيف حاسوبك.

• الموقع Scumware.com: هو موقع مبسط يعتمد الإنجليزية اليسيرة، ويتضمن توجيهات حول كيفية اكتشاف البرامج الخبيثة ومواد الإعلانات وإزالتها.

• الموقع MajorGeeks.com: به معلومات عن البرامج الخبيثة للمستخدم الأكثر خبرة.

فإن لم تكن متأكدا مما إذا كان ملف معين خبيثاً، يمكنك إرساله إلى مواقع مختلفة مثل: www.virustotal.com) VirusTotal) وvirusscan.jotti.org

وكلاهما يستخدم أكثر من عشرة محركات فحص لتقرير طبيعة الملف. كما يمكنك إرفاق هذا الملف برسالة إلكترونية وإرسالها إلى العنوان scan@virustotal.com مع وضع الكلمات SCAN في سطر العنوان الخاص بها. وستتلقى تقريراً بريدياً إلكترونيا حول نتيجة الفحص.

منتديات النقاش وموارد التنزيل:

• www.wilderssecurity.com) Wilders Security Forums)
• castlecops.com/forums.html) ComputerCops forums)
• boards.cexx.org) cexx.org Message Boards)





أرجو أن تكونوا استفدتم بقراءة هذا الكتاب ولتدعوا الله لي بظهر الغيب

ولأي استفسار بالرجاء التواصل أو مراسلتي عبر الرابط التالي :-

E mail :- MostafaDigital@yahoo!.com

ولكم تحياتي

م/ مصطفى عبده توفيق محمد